GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 708
TO BE ANSWERED ON: 25.07.2025

REGULATION OF GENERATIVE AI TOOLS

708. SHRI K.R. SURESH REDDY:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether Government is aware of any cybersecurity issues with generative Artificial Intelligence (AI) tools being used by citizens in India;
(b) if so, the details thereof;
(c) whether Government plans to bring any set of rules/guidelines to regulate the use of such generative AI tools keeping in mind the security issues; and
(d) if so, the details thereof, if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): Government remains conscious of the cyber threats and challenges arising from emerging technologies such as AI. India’s AI strategy is based on the Hon’ble Prime Minister's vision to democratize the use of technology. It aims to address India-centric challenges, create economic and employment opportunities for all Indians.

India’s AI strategy:

India’s AI strategy aims to position India as a global leader in AI. Established in 2024, IndiaAI mission is a strategic initiative to develop a robust and inclusive AI ecosystem through its seven key pillars.

- One of the seven key pillars is “Safe and Ethical AI”, which focuses on ensuring secure, trustworthy, and responsible use of AI technologies.
- Eight (8) Responsible AI projects selected from leading academic institutions, start-ups, and civil society. Details available at Annexure I.
- These projects aim to develop indigenous governance tools and safeguards. Special focus on developing tools factoring in India’s linguistic diversity.

Legal provisions under IT Act, 2000:

- Section 66C (Punishment for identity theft) deals with misinformation, deepfakes, cheating by personation or identity theft.
- Section 66D of the IT Act criminalizes the use of computer resources for cheating by personation.
- Section 66E prescribes the punishment for capturing and publishing or transmitting the image of a private area of any person without his or her consent.

- Section 67A and 67B make publishing or transmitting obscene material for instance, which could be generated by using deepfake technology a punishable offence.

Legal provisions under Bharatiya Nyay Sanhita, 2023:

- Section 111 of the BNS punishes the commission of any continuing unlawful activity including economic offence, cyber-crimes, by any person or a group of persons, either as a member of an organised crime syndicate or on behalf of such syndicate.
- Several other sections under the BNS also deal with cyber-crimes like cheating or cheating by personation such as sections 318 (Cheating), 319 (cheating by personation), 353 (public mischief), 356 (defamation).

Digital Personal Data Protection Act, 2023

It casts obligations on Data Fiduciaries to safeguard digital personal data, holding them accountable, while also ensuring the rights and duties of Data Principals.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021")

- The IT Rules cast specific legal obligations on intermediaries, including social media intermediaries and platforms, to ensure their accountability towards safe and trusted internet including their expeditious action towards removal of the prohibited misinformation, patently false information and deepfakes.
- In case of failure of the intermediaries to observe the legal obligations, they are liable for consequential action or prosecution as provided under the extant laws.
- Under the IT Rules 2021, there is a provision for a grievance redressal mechanism by the intermediaries which inter-alia provides 24 hours of timelines for any grievances relating to morphed or artificially generated images affecting the victim.
- If not satisfied with the grievance redressal, aggrieved persons can approach Grievance Appellate Committee.
- Ministry of Home Affairs has launched a dedicated portal to report cybercrimes [cybercrime.gov.in] and has also started a toll-free number 1930.

Indian Computer Emergency Response Team (CERT-In) Advisories/Guidelines:

- An advisory on safety measures to be taken to minimize the adversarial threats arising from Artificial Intelligence (AI) based applications was published in May 2023. It is available at the link https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2023-0015.
- Certified Security Professional in Artificial Intelligence (CSPAI) program launched by CERT-In and SISA in September 2024.
- Advisory depicting best practices for effective and responsible use of Generative AI solutions published in March 2025.
- Technical guidelines for Bill of Materials (BOM) for Software, Hardware, Artificial Intelligence and Quantum and Cryptography requirements have been issued for enhancing the security and transparency of software and emerging technologies supply chains in July 2025.

- The CSPAI program equips cybersecurity professionals with the skills to secure AI systems, proactively address AI-related threats, and ensure trustworthy AI deployment in business environments.

Government has constituted an Advisory Group on AI for India-specific regulatory AI framework under the chairmanship of Principal Scientific Advisor (PSA) to Prime Minister. It has members from diverse stakeholders from academia, industry and government.

****

Annexure I

Details of projects selected against the first Expression of Interest (EoI) floated under the **Safe and Trusted AI Pillar**

Name Of the Theme	**Selected Applicant**	**Title Of the Project**	**About the Project**
Machine Unlearning	IIT Jodhpur	Machine Unlearning in Generative Foundation Models	To development novel method for targeted unlearning in open-source generative foundation models while minimising negative impact on overall model performance.
Synthetic Data Generation	IIT Roorkee	Design and Development of Method for Generating Synthetic Data for Mitigating Bias in Datasets; and Framework for Mitigating Bias in Machine Learning Pipeline for Responsible AI	To develop the algorithm and method for handling the bias at the model training and in-processing stage of ML model development
AI Bias Mitigation Strategy	National Institute of Technology Raipur	Development of Responsible Artificial Intelligence for Bias Mitigation in Health Care Systems	To develop responsible AI algorithms that reduce biases in medical system applications, image

Name Of the Theme	**Selected Applicant**	**Title Of the Project**	**About the Project**
			analysis, and diagnostic decisions
Explainable AI Framework	DIAT Pune and Mindgraph Technology Pvt. Ltd.	Enabling Explainable and Privacy Preserving AI for Security	Create AI models that provide accurate and interpretable results for human activity analysis for effective security in crowded environment.
Privacy Enhancing Strategy	IIT Delhi, IIIT Delhi, IIT Dharwad and Telecommunication Engineering Center (TEC)	Robust Privacy-Preserving Machine Learning Models	To develop robust distributed/federated learning algorithms which perform well in an adversarial environment susceptible to attacks
AI Ethical Certification Framework	IIIT Delhi and Telecommunication Engineering Center (TEC)	Tools for assessing fairness of AI model	To develop a three-step certification process involving bias risk assessment, processing for metrics, and bias testing to ensure fairness for AI Systems in the Indian context
AI Algorithm Auditing Tool	Civic Data Labs	ParakhAI - An open-source framework and toolkit for Participatory Algorithmic Auditing	The proposed framework and toolkit will enable involving citizens in the responsible design, development, and deployment of algorithmic decision-making systems.

Name Of the Theme	**Selected Applicant**	**Title Of the Project**	**About the Project**
AI Governance Testing Framework	Amrita Vishwa Vidyapeetham and Telecommunication Engineering Center (TEC)	Track-LLM, Transparency, Risk Assessment, Context & Knowledge for Large Language Models	To identify and address the specific gaps in the existing governance testing frameworks related to LLM;s downstream use-case and deployment

******